ABSTRACT

DETECTION ANALYSIS OF MALICIOUS ACTIVITY USING ANOMALY-BASED DYNAMIC MALWARE ANALYSIS METHOD

By

DAMAR AURIGA DANISWARA

1202150007

With the advance in technology and broader use of internet, comes a greater threat in cyber-crime. One of such that can potentially harm individuals or companies is malware attack. Malware is a software that is thoroughly designed for data theft, data manipulation and full access control of the infected hosts. According to av-test.org, malware attacks have increased to 902.82 million malwares in 2019 and caused losses of up to 11.7 million US dollars. One of the ways to tackle these problems is to design a malware detection analysis which aims to detect malicious activity carried out by malware during the time it is executed. The analysis was carried out using anomaly-based dynamic malware analysis method, namely by running malware samples in an environment that was designed in Virtual Machine. Anomaly is a pattern that is not in accordance with the normal pattern of a program. This study was conducted by testing 10 randomly downloaded malware samples which were then analyzed using three different malware-detection tools. Anomalies from malware are tracked from suspicious activity, registry accessed and API calls by malware samples. The test results are then matched with malicious activity data sets in the form of a collection of APIs called by malware samples, which shows that 40% of the 10 samples tested proven to be malware.

***Keyword** : malware, malware analysis, cyber-crime, dynamic malware analysis, anomaly*